第１節

申請者の電子証明書の取得

■申請者の電子証明書の取得

申請者と法務省とがインターネットを介してオンラインでデータのやり取りをする際には、
法務省側は、申請者の真正性、つまり、相手方は本当の申請者かどうかを検証する必要があります。
この申請者の真正性は、次の２点により確保されます。

・申請者の電子証明書
　申請者に関する情報と申請者の公開鍵に対し、認証局が電子署名したものです。
　認証局が電子署名することによって、公開鍵が真に申請者のものであることが証明されます。

・申請者の電子署名
　申請者は、申請書に自分の秘密鍵を使って電子署名します。
　法務省は、この電子署名に対して、申請者の電子証明書の中にある公開鍵を施すことによって、
　申請書が本当に申請者からのものであるかどうかを検証できます。

まず、申請者は、自分の電子証明書（自分の公開鍵の真正性を証明してくれる電子データ）を取得する必要があります。取得する手段はいろいろありますが、ここでは、地方公共団体による公的個人認証サービスを利用します。

公的個人認証サービスでは、住民に対し電子証明書を交付し、住民基本台帳カード（以後、住基カードと呼ぶことにします。）の IC に格納してくれます。

公的個人認証サービスにおける電子証明書の発行手続きは、次のようになります。

（１）次のものを持って、居住地の市町村役場窓口に行きます。
　　・住基カード（まだ作成していない場合には、市町村役場窓口で作成を依頼します。）
　　・公的な身分証明書（運転免許証や保険証等。写真付き住基カードならそれだけで OK。）
　　・電子証明書発行手数料（500 円）

（２）電子証明書新規発行申請書を提出するとともに、身分証明書を提示します。

（３）鍵ペア生成装置に住基カードをセットし、鍵ペアを住基カードに書込みます。
　　鍵ペアとは、秘密鍵と公開鍵のペアです。
　　その際、パスワード（アルファベットと数字の組み合わせで４文字以上 16 文字以内）を設定
　　します。このとき設定するパスワードは、電子文書に、秘密鍵を使って電子署名をする際に
　　必要となりますので、絶対に忘れないようにし、かつ、他人に知られないようにして下さい。
　　この時点で、住基カードの IC には、基本４情報（氏名、生年月日、性別、住所）と、
　　鍵ペア（公開鍵と秘密鍵）が格納されます。

（4）住基カードを市町村窓口役場の職員に渡し、

上記の格納情報に対し、認証局（この場合は、都道府県知事）の秘密鍵（正式には、「発行者署名符号」）により、電子署名を施してもらいます。

これによって、住基カードの IC 内に、電子証明書が格納されることになります。

電子証明書の実体は、住民の基本４情報と公開鍵に、都道府県知事が電子署名を施した電子データです。

この時点で、住基カードの IC には、次のものが格納されます。

・電子証明書（利用者の基本４情報と公開鍵に、都道府県知事が電子署名した電子データ）

・利用者の秘密鍵

・都道府県知事の自己署名証明書

このような、秘密鍵が格納された住基カードは、実印と同等のものですので、厳重に管理しなければなりません。

（5）市町村役場窓口で、発行手数料を支払い、次のもの（全４点）を受け取ります。

・住基カード

・電子証明書の写し（紙切れ 1 枚）

住基カードの IC に格納されている利用者情報をプリントアウトしたものです。

・電子証明書の利用のご案内（紙切れ 1 枚）

この紙切れには、次の事項が記載してあります。

・公的個人認証サービスブリッジ認証局の自己署名証明書のフィンガープリント

・都道府県知事（都道府県認証局）の自己署名証明書のフィンガープリント

PKI に疎い市町村役場窓口では、渡さない場合もありますが、その場合には請求して下さい。

尚、都道府県認証局の自己署名証明書のフィンガープリントは、次の Web ページでも公開されております。（www.jpki.go.jp/cps/ca_fingerprint.pdf）

・使用可能な IC カードリーダライタ機種名の一覧表

地方公共団体によって、住基カードの仕様が異なるので、

それを読み書きするための IC カードリーダライタも、各地方公共団体によって異なります。

利用者は、自分が居住する地方公共団体の住基カードを読み書きできる IC カードリーダを購入する必要があります。

PKI に疎い市町村役場窓口では、渡さない場合もありますが、その場合には請求して下さい。

一覧表の文字は、極めて小さく読み難いので、市町村役場の窓口で拡大コピーしてもらうとよいでしょう。

■ JRE：Java Runtime Environment（Java 実行環境）のインストール

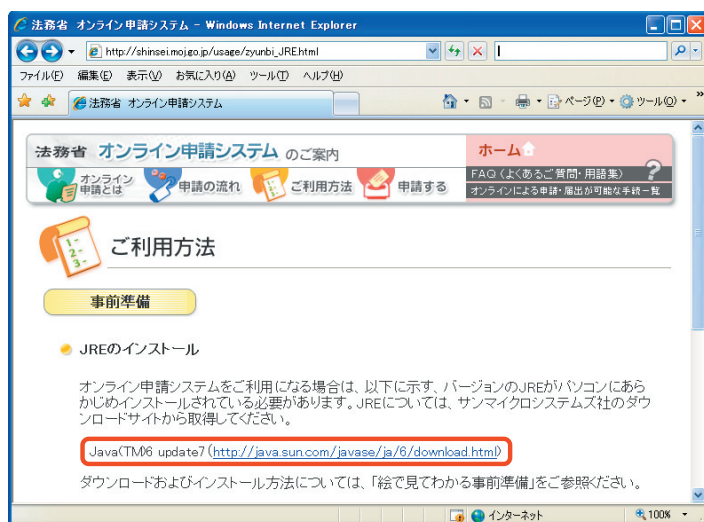
利用者クライアントソフトと法務省オンライン申請システムは、JRE というプログラム上で動作します。
JRE は、サンマイクロシステムズ社の Web サイトにアクセスし、ダウンロードした後、申請者のパソコンにインストールする必要があります。

まず、オンライン申請に使用するパソコン内に、既に JRE がインストールされていないかどうかを調べます。
「スタート」→「コントロールパネル」（カテゴリ表示）を選択します。

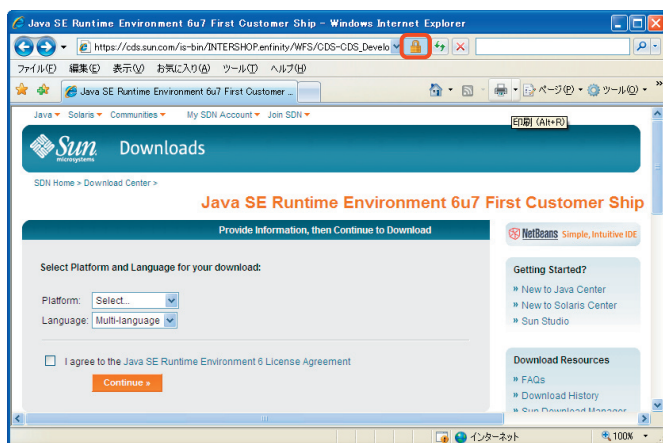
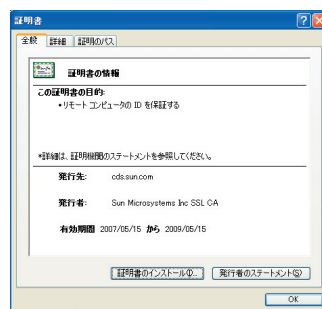
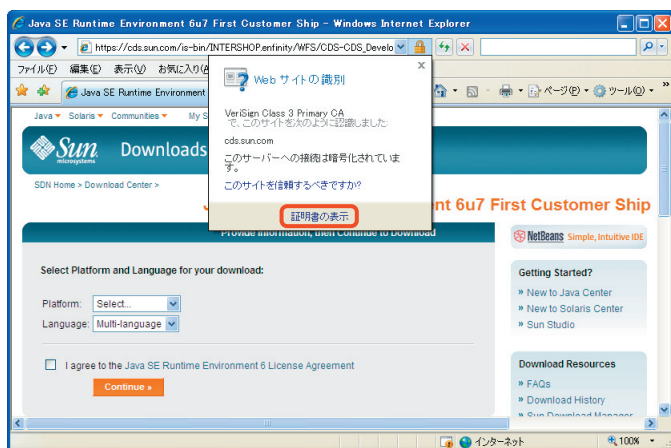
「プログラムの追加と削除」をクリックします。

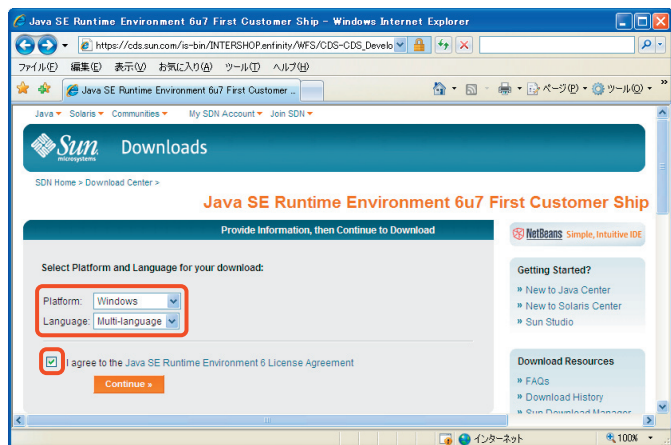
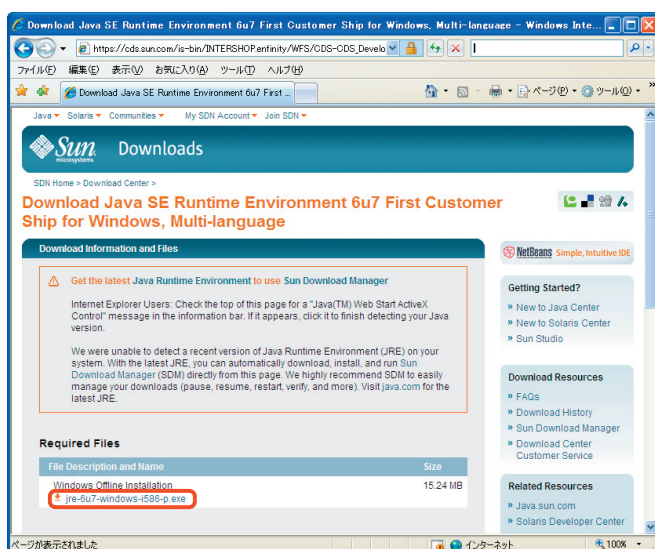
表示されたプログラム群の中に、「Java (TM) 6 Update 7」というプログラムがあるかどうか調べます。
もし、該当するプログラムがあれば、これ以降の JRE のインストール手続きは不要です。
「Java (TM) 6 Update 7」以外の、「Java」もしくは「J2SE」で始まるプログラムがあった場合には、
それらを削除し、以降の手続きにより、新たに、「Java (TM) 6 Update 7」をインストールする必要があります。

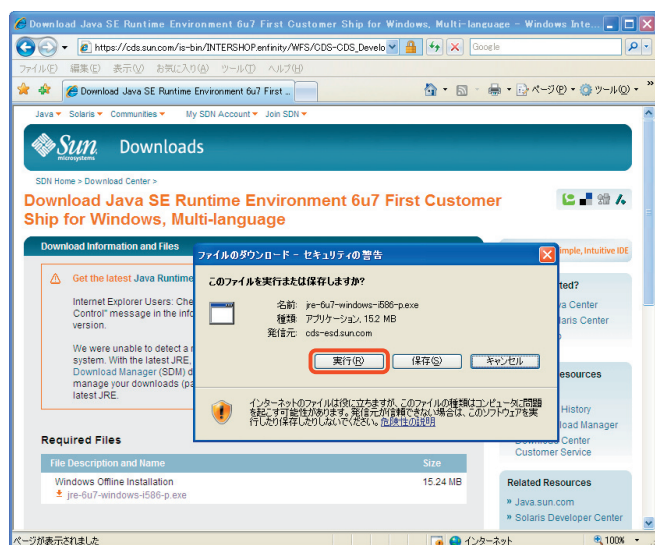
JRE をダウンロードするために、法務省のリンク元 Web ページにアクセスします。
(http://shinsei.moj.go.jp/usage/zyunbi_JRE.html)

「Java(TM) 6 update 7」と記載された部分をクリックします。

なぜ JRE なのか
国家機関が運営する申請システムが、特定の私企業の OS にのみ依存するのは、国家政策上、好ましくないから。OS と申請システムとの間に JRE を挟み込めば、特定の OS にのみ依存しない申請システムにすることができる。

申請システム
JRE
OS

OS: Windows , Linux , UNIX , Mac OS, etc

URL 欄右の「鍵アイコン」は SSL：Secure Socket Layer というプロトコルにより、通信が安全に行われることを示しています。
利用者側のアカウント情報を送る場合や、相手のサイトからプログラムをダウンロードしようとするときには、「鍵アイコン」がかかっているかどうかを必ず確認する必要があります。
念のため「鍵アイコン」をクリックして、サーバ証明書（SSL 暗号化通信する際に、サーバ側が送ってくる証明書）を表示させます。

証明書の各タブをクリックして、内容をよく確認します。

証明書の内容に問題が無ければ、「OK」をクリックして証明書を閉じ、元のダウンロードページに戻ります。

プルダウンリストで、
Platform に Windows を、
Language に Multi-language を選択し、
I agree … にチェックを入れ、
「Continue」をクリックします。

「jre-6u7-windows-i586-p.exe」をクリックします。

「ファイルのダウンロード – セキュリティの警告」が現れます。

「実行」をクリックします。

▶「実行」或は「開く」と「保存」との違い

・「実行」或は「開く」をクリックした場合

プログラムの場合は、インストーラのダウンロードが実行され、続いて、(圧縮されている場合には)解凍が行われ、インストーラによりプログラム本体のインストールが行われます。

書類や証明書の場合は、ダウンロードが実行され、続いて、それらが開かれます。

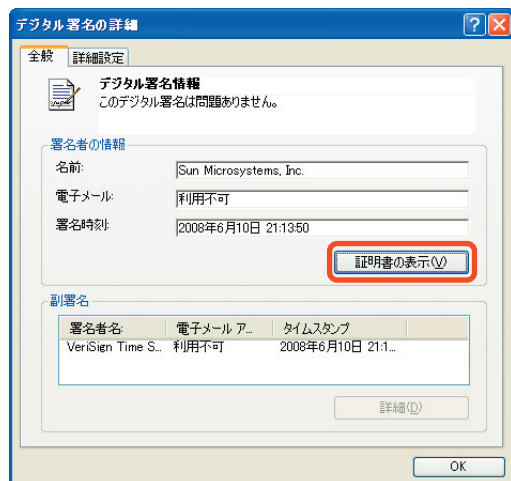
・「保存」をクリックした場合

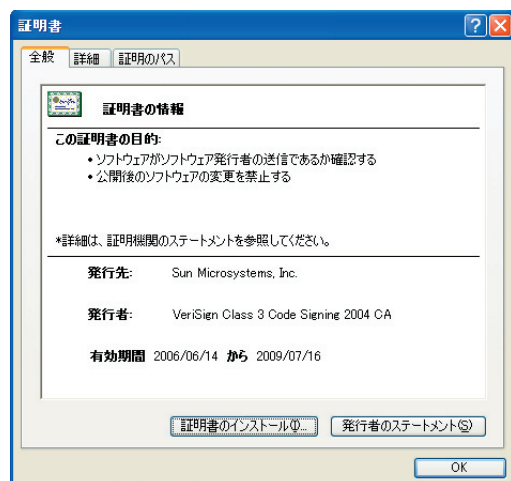
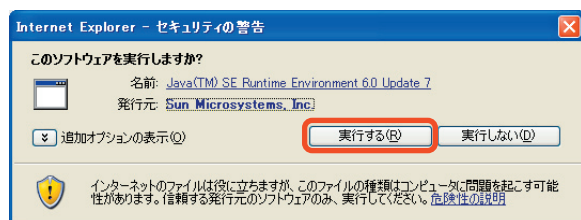
プログラムの場合は、一旦、インストーラが保存され、そのインストーラを利用者がダブルクリックすることによって、プログラム本体のインストールが開始されます。

書類や証明書の場合は、ダウンロードの後、保存され、それらのアイコンを利用者がダブルクリックすることによって開かれます。

ダウンロードが開始され、やがてダウンロードを終えると、「Internet Explorer - セキュリティ警告」が現れます。

発行元名をクリックし、
コード署名（ソフトウエアに施された作成者の電子署名）を確認します。

プログラムの発行元の「デジタル署名の詳細」が表示されます。

改ざんされたコードをインストールしてしまうと大変です。また、改ざんの有無も、ドキュメントのそれに比べ（人間が見たり読んだりして）気付き難いので、
コードの真正性の検証は、念入りに行う必要があります。

「証明書の表示」をクリックし、
コード署名証明書（コード署名に付された証明書。そのコードの真正性を確認するために用いる。）を表示させます。

各タブをクリックして、証明書の内容をよくチェックした後、問題が無ければ、元の「Internet Explorer - セキュリティ警告」に戻ります。

「実行する」をクリックします。

Java セットアップ画面が現れます。

使用許諾契約を表示させ、一応、目を通した後、「同意する」をクリックします。

Java セットアップの進捗状況を示す画面が現れます。

やがて、インストールが終わり、インストール完了画面が現れます。

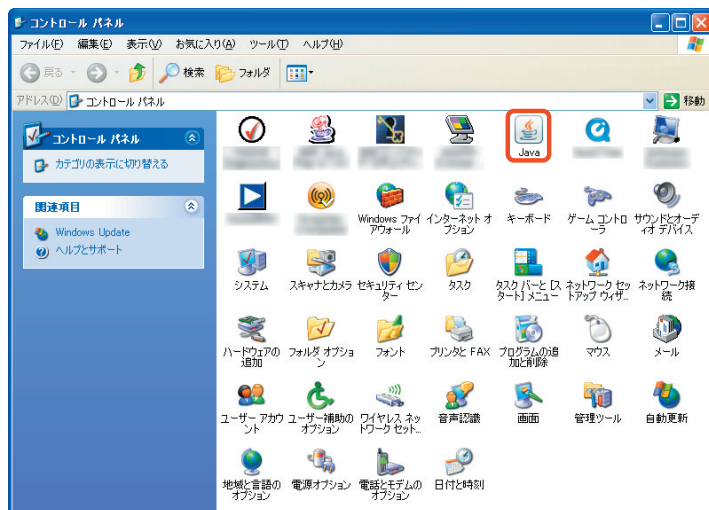
「完了」をクリックします。

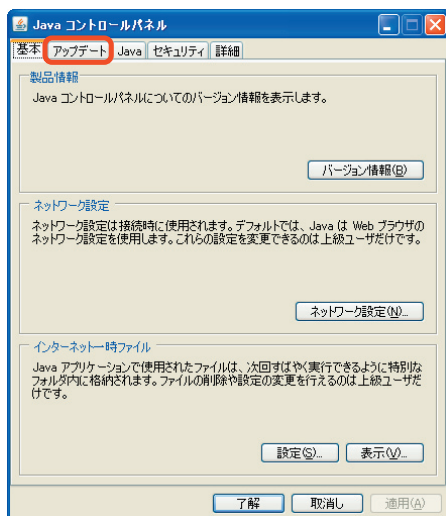
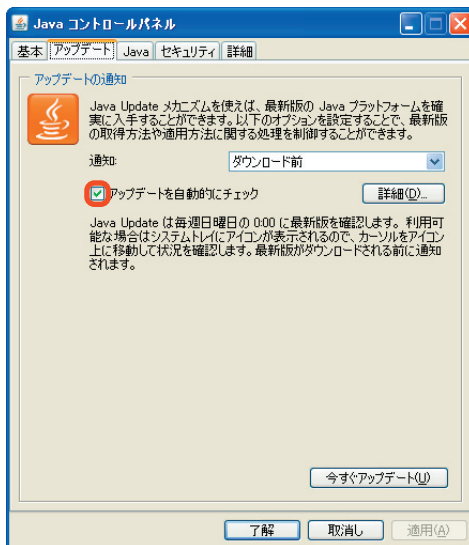
■ JREの自動更新設定の解除

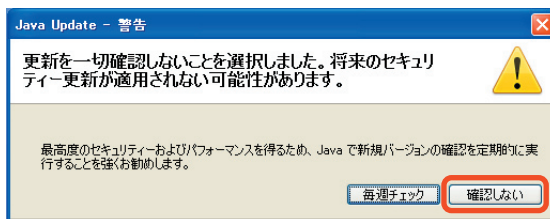
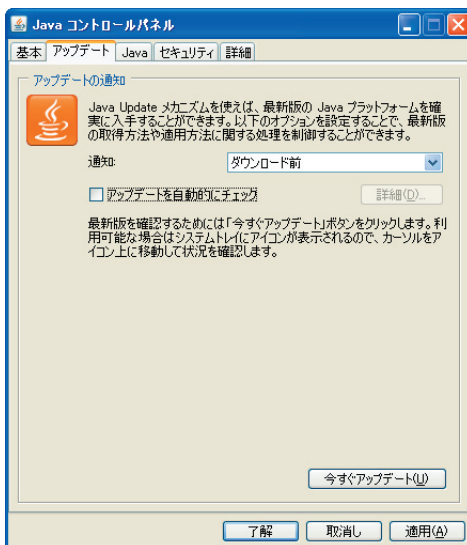
JREには、利用者がインターネットにアクセスした際に、利用者のパソコンにインストールされているJREのバージョンを調べ、最新のバージョンのものでなければ、最新のものに自動的にアップデートするプラグインが組込まれています。

しかし、法務省オンライン申請システムを利用する場合には、その動作の確実性を確保するために、
特定のバージョンのJREに維持しておく必要があります。

そのために、インストールしたJREプラグインの自動更新機能は解除しておきます。

「スタート」→「コントロールパネル（クラシック表示）」を選択します。

「Java アイコン」をダブルクリックします。

「Java コントロールパネル」が現れます。

「アップデート」タブをクリックします。

「アップデートを自動的にチェック」のチェックマークを外します。

警告メッセージが現れます。

「確認しない」をクリックします。

「適用」をクリックし、
続いて、「了解」をクリックします。

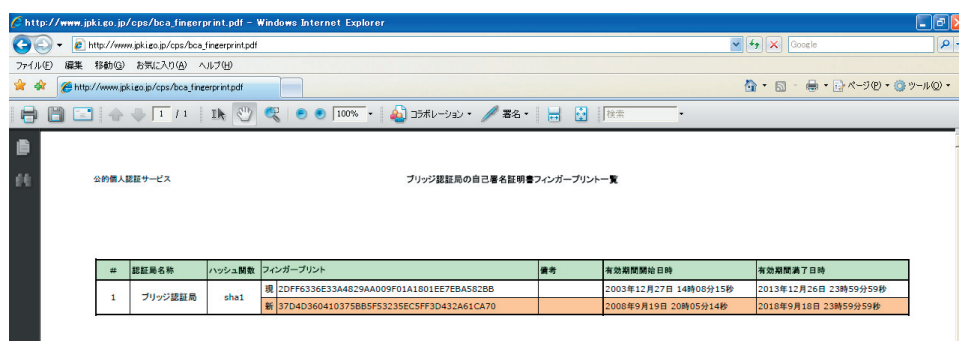
■ IC カードリーダライタの準備

電子証明書の交付を受けるときに、通常、市町村役場窓口で、利用可能な IC カードリーダのリストを手渡されますが、市町村によっては、手渡されない場合もあります。
従って、ここでは、公的個人認証サービスの Web サイトにアクセスし、利用可能な IC カードリーダを調べた上で、IC カードリーダライタを購入する事にしましょう。

まず、公的個人認証サービスポータルサイトの「適合性検証済 IC カードリーダライタ一覧」にアクセスします。
(http://www.jpki.go.jp/rwinfo/html/rwinfo_top.html)

該当する都道府県をクリックします。

市町村を選択するページが現れ、該当する市町村をクリックすると、その市町村で発行されている住基カードの読み取りに使用できる IC カードリーダライタの一覧（PDF 書類）が表示されます。
その中から、自分のパソコンのオペレーティングシステムで使用できる IC カードリーダライタを選択します。

次に、「公的個人認証サービス対応 IC カードリーダライタ普及促進協議会」のサイトにアクセスします。
(http://www.jpki-rw.jp/list/index.html)

このサイト上で、最寄りの販売店を検索して調べた後、直接出向いて購入するか、
或は、各メーカ等の通販サイトに移動して、インターネット上で購入手続きをとります。
購入した後、取扱説明書にしたがって、IC カードリーダライタのドライバをパソコンにインストールします。

■利用者クライアントソフトのインストール

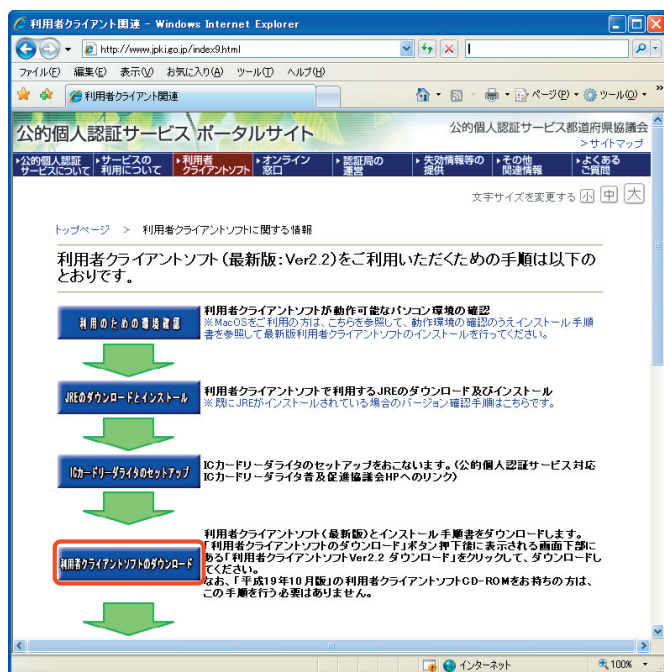
利用者クライアントソフトは、住基カード（IC カード）を基に、利用者が各種の操作をするためのものです。
当初、利用者クライアントソフトは、電子証明書の交付の際に、CD の形で市町村役場窓口で手渡されましたが、
現在は、公的個人認証サービスポータルサイトからダウンロードするようになっております。
CD の形で市町村役場窓口で手渡される分には、偽の「利用者クライアントソフト」を掴まされる心配は、ほとんど無いのですが、インターネットを介したダウンロードでは、偽のサイトからマルウエア（悪事を働くソフトウエア）を掴まされたり、途中ですり替えられる恐れも出てくるので、細心の注意が必要です。

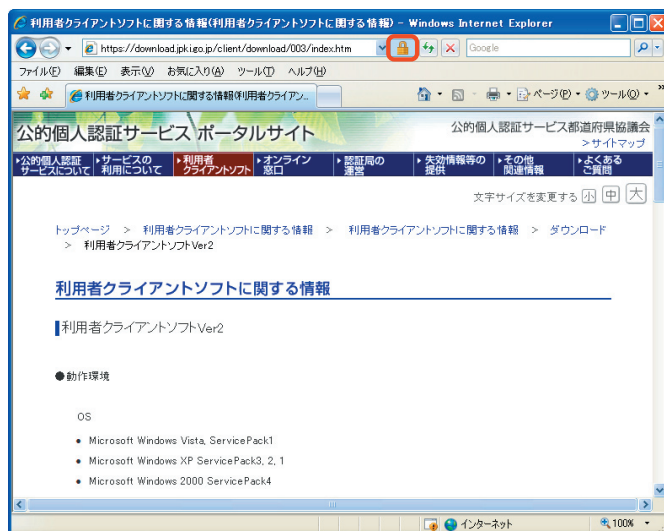
利用者クライアントソフトは、先にダウンロードした JRE 上で動作し、その JRE はキーストア（暗号通信や認証を行うための公開鍵を格納しておく領域）を有し、利用者クライアントソフトをインストールする過程で、
そのキーストアに、公的個人認証サービスブリッジ認証局（BCA：Bridge CA）の自己署名証明書（の公開鍵）の登録が要求されます。
当該フィンガープリントは、市町村役場窓口で、電子証明書とともに渡される紙切れに記載されておりますが、
Web 上では、次のページで公開されております。(http://www.jpki.go.jp/cps/bca_fingerprint.pdf)

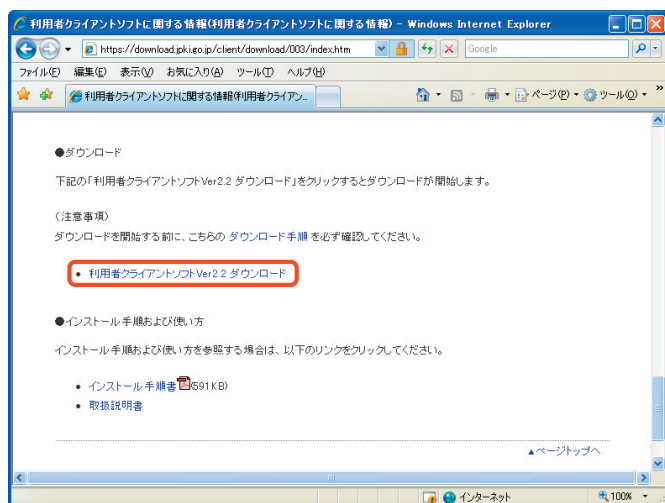
#	認証局名称	ハッシュ関数	フィンガープリント	備考	有効期間開始日時	有効期間満了日時
1	ブリッジ認証局	sha1	現 2DFF6336E33A4829AA009F01A1801EE7EBA582BB		2003年12月27日 14時08分15秒	2013年12月26日 23時59分59秒
			新 37D4D360410375BB5F53235EC5FF3D432A61CA70		2008年9月19日 20時05分14秒	2018年9月18日 23時59分59秒

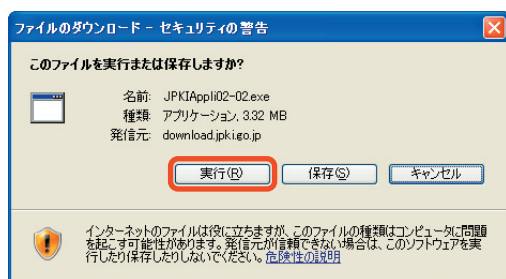
一応、このページをプリントアウトしておきます。

利用者クライアントソフトをダウンロードするため、公的個人認証サービスポータルサイトへアクセスします。
(http://www.jpki.go.jp/index.html)

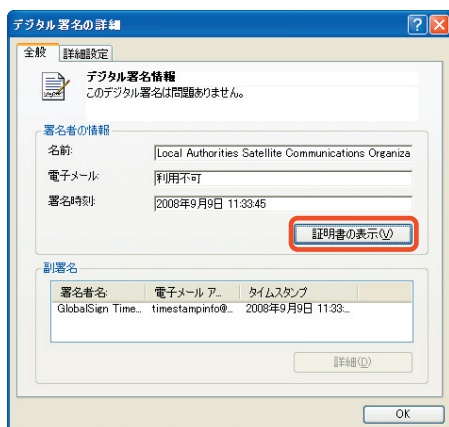
「利用者クライアントソフト ダウンロードとインストール」をクリックします。

「利用者クライアントソフトのダウンロード」をクリックします。

「利用者クライアントソフトに関する情報」というページが現れます。

プログラムをダウンロードしようとしているので、当然、ここからはSSL暗号通信です。念のために「鍵アイコン」をクリックして「証明書の表示」を選択して証明書を表示させます。

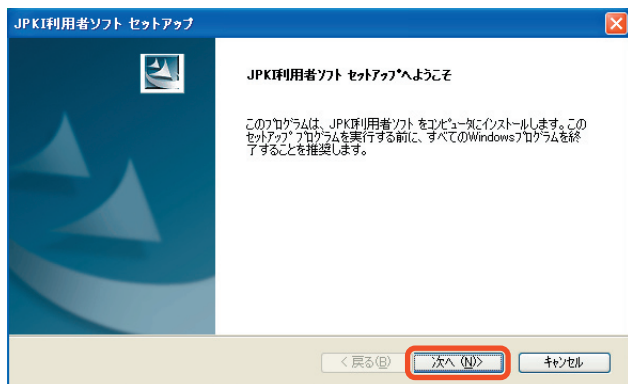
証明書の各タブをクリックして、内容をよく確認します。

サーバ証明書の内容に問題が無ければ、元の画面を下方にスクロールして、「利用者クライアントソフト Ver2.2 ダウンロード」と記載された部分をクリックします。

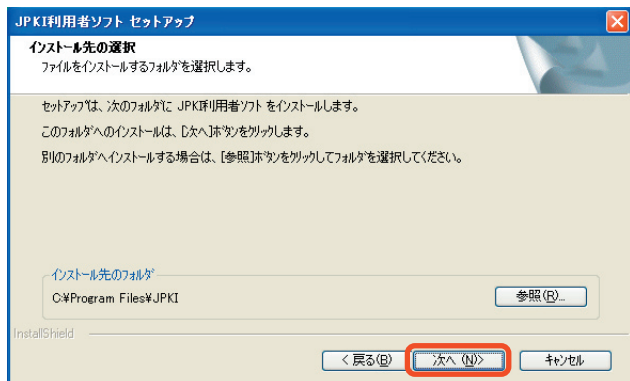
「ファイルのダウンロード – セキュリティの警告」が現れます。

「実行」をクリックします。

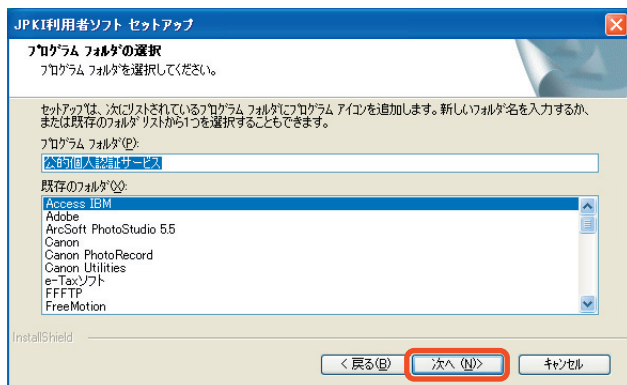
ダウンロードが開始され、完了すると、ソフトウエアを実行するかどうか聞いてきます。

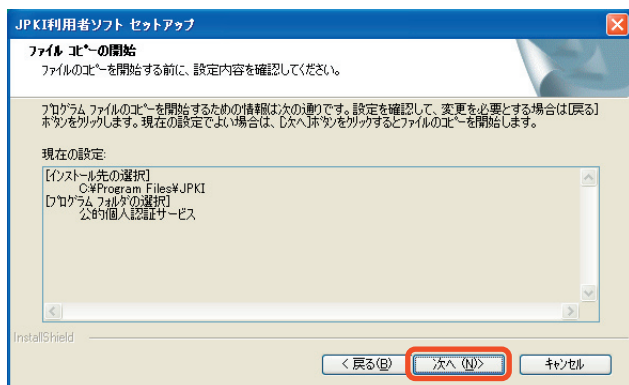
念のために、発行元名をクリックし、コード署名とその証明書を確認しておきましょう。

「証明書の表示」をクリックし、コード署名証明書を表示させた後、各タブをクリックして、内容をよく確認し、問題が無ければ、元の「Internet Explorer – セキュリティの警告」に戻ります。

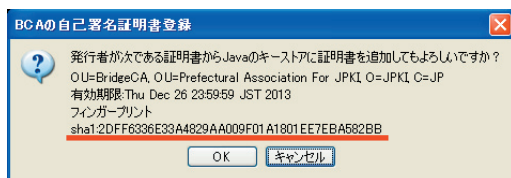
「実行する」をクリックします。

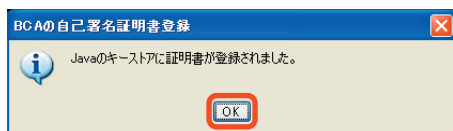
利用者クライアントソフト（JPKI 利用者ソフト）のセットアップ画面が現れます。

「次へ」をクリックします。

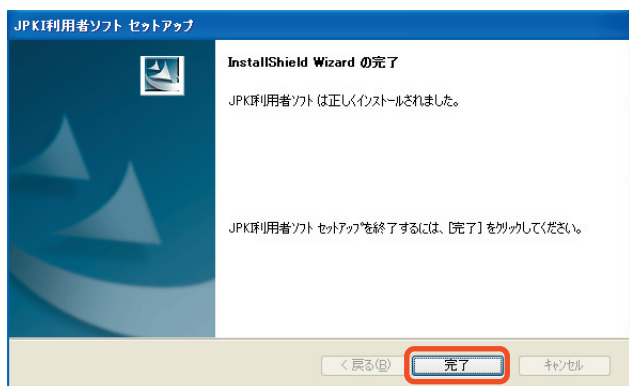
JPKI 利用者ソフトのインストール先を聞いてきます。

別のインストール先にしたいのでなければ、そのまま「次へ」をクリックします。

プログラムを格納するフォルダ名を聞いてきます。

別のフォルダ名を指定したいのでなければ、そのまま「次へ」をクリックします。

設定状況の確認をしてきます。

「次へ」をクリックします。

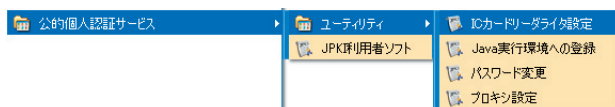
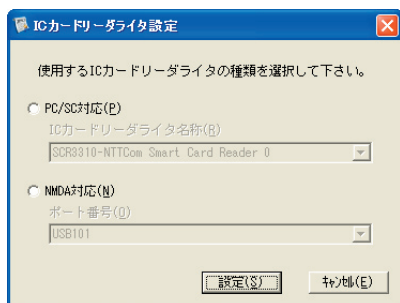
いくつか「質問」等のダイアログボックスが現れますが、全て「はい」をクリックすると、
「BCA の自己署名証明書登録」というダイアログボックスが現れます。
尚、ここで言う BCA は、政府認証基盤のブリッジ認証局ではなく、公的個人認証サービスブリッジ認証局です。

先に、市町村役場窓口で手渡された「電子証明書の利用のご案内」、或は、Web 上からダウンロードしプリントアウトした、公的個人認証サービスブリッジ認証局のフィンガープリントと比較し、完全に一致しているならば「OK」をクリックします。

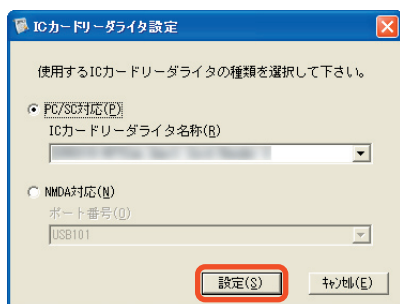
Java のキーストアに証明書が登録された旨のメッセージが現れます。

「OK」をクリックします。

セットアップ完了画面が現れます。

「完了」をクリックします。

■ IC カードリーダライタの設定

パソコンに、利用者クライアントソフト（JPKI 利用者ソフト）をインストールし終えたので、
次は、当該ソフトに、扱うべき IC カードリーダライタのドライバインタフェースの設定を行う必要があります。

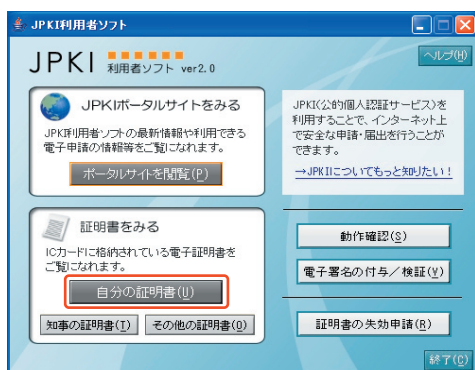
パソコンに IC カードリーダライタを接続し、「スタート」→「すべてのプログラム」→「公的個人認証サービス」→「ユーティリティ」→「IC カードリーダライタ設定」を選択します。

「IC カードリーダライタ設定」ダイアログボックスが現れます。

市町村役場窓口で手渡された IC カードリーダライタ機種名一覧表で、使用機種のドライバインタフェース（PC/SC か NMDA）の別を調べ、該当するラジオボタンを選択します。
尚、PC/SC とか NMDA というのは IC カードの規格名です。

・PC/SC：Personal Computer / Smart Card
・NMDA：New Media Development Association

プルダウンメニューより、先にインストールした IC カードリーダライタのドライバを選択し、「設定」をクリックします。

JPKI 利用者クライアントソフトのユーティリティには、IC カードリーダライタ設定の他に、
次のようなものがあります。

・Java 実行環境への登録
　JPKI 利用者ソフトや JPKI ブリッジ認証局自己署名証明書を Java 実行環境（JRE）に登録します。
・パスワードの変更
　住基カード（IC カード）に設定したパスワードを変更できます。
・プロキシ設定
　プロキシサーバを介して外部のインターネットと接続するように設定できます。

■利用者クライアントソフトの利用

IC カードリーダライタをパソコンに接続し、住基カードを挿入した後、
「スタート」→「すべてのプログラム」→「公的個人認証サービス」→「JPKI 利用者ソフト」を選択すると、
次のダイアログボックスが現れます。

「自分の証明書」をクリックします。

JPKI 利用者ソフトは、見ての通り、ボタンの数だけ色々な事ができます。

・JPKI のポータルサイトをみる：　JPKI のポータルサイトにアクセスできます。

・証明書をみる：

住基カードの IC 内に格納された利用者の証明書や知事の自己署名証明書の内容を見る事ができます。
また、利用者のパソコンに格納された他の証明書の内容も見る事ができます。

・動作確認：　IC カードリーダライタの動作確認ができます。

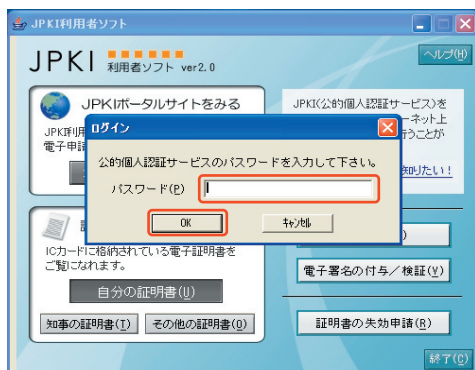
・電子署名の付与 / 検証：

利用者のパソコン内の電子文書に、利用者の電子署名を付与することができます。
また、電子文書に付与された電子署名が、利用者等のものであるかどうかを検証できます。

・証明書の失効申請：　オンラインで失効申請ができます。

失効申請（と共に市町村窓口に失効届出）を行うのは、例えば、次のような場合です。

- ・電子証明書の利用をやめる時
- ・住基カード（IC カード）を紛失したり、盗まれたりしたとき
- ・住基カードの IC が破損したり、故障したとき
- ・住基カード（IC 内の利用者の秘密鍵）が他人に不正使用されたり、そのおそれが生じたとき

ログインダイアログボックスが現れ、パスワードの入力を求められます。

市町村役場に設置された鍵ペア生成装置で、住基カード内に鍵ペアを作成する際に設定したパスワードを入力し、「OK」をクリックします。

住基カードの IC 内に格納された利用者の電子証明書の内容が表示されます。

証明書表示
公的個人認証サービス　利用者の電子証明書
基本情報　詳細情報
氏名(N)
生年月日(T)
性別(S)
住所(A)
発行年月日(Y)　平成19年 月 日
有効期間の満了日(E)　平成22年 月 日
発行者(I)　知事
ファイル出力(F)　有効性確認(V)
電子証明書の有効性確認は行われていません。

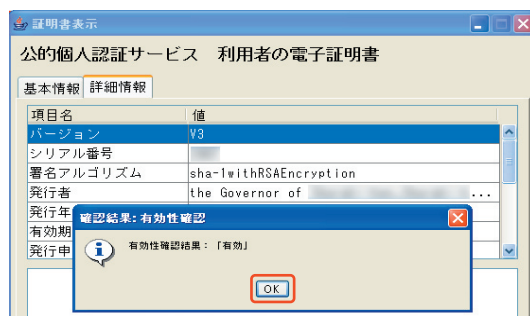
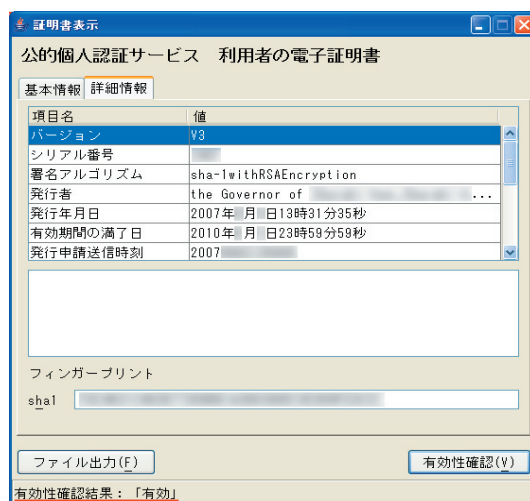
「詳細情報」タブをクリックします。

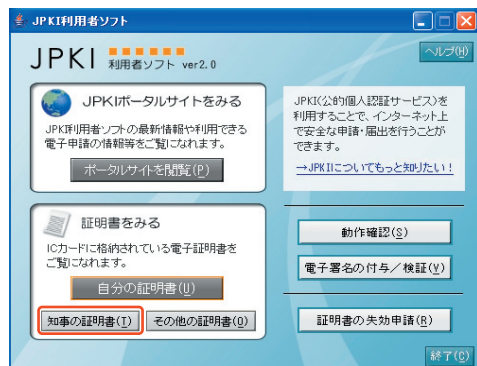
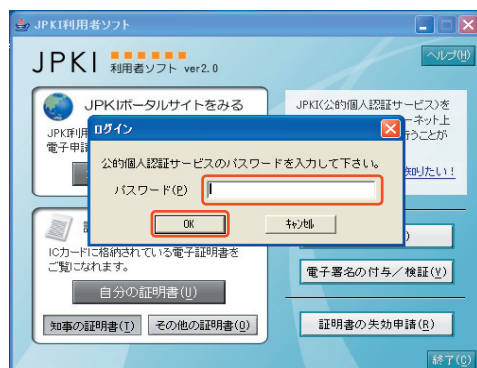
証明書表示
公的個人認証サービス　利用者の電子証明書
基本情報　詳細情報

項目名	値
バージョン	V3
シリアル番号	
署名アルゴリズム	sha-1withRSAEncryption
発行者	the Governor of ...
発行年月日	2007年 月 日13時31分35秒
有効期間の満了日	2010年 月 日23時59分59秒
発行申請送信時刻	2007

フィンガープリント
sha1
ファイル出力(F)　有効性確認(V)
電子証明書の有効性確認は行われていません。

左下に、「電子証明書の有効性確認は行われていません。」と記載されているので、「有効性確認」をクリックします。
尚、有効性確認はネットワークを介して公的個人認証サービスブリッジ認証局に対して問い合わせが行われるので、パソコンをネットワークに接続しておく必要があります。
その際に、相手のサイトが本当に公的個人認証サービスブリッジ認証局かどうかを検証するために、先に JRE のキーストアに登録した、「BCA の自己署名証明書」が使用されます。

ログインダイアログボックスが現れるので、パスワードを入力し、「OK」をクリックします。

「OK』をクリックします。

左下に、「有効性確認結果：「有効」と表示されていることを確認し、証明書表示のウインドウを閉じます。

次に、利用者の電子証明書の発行者である都道府県知事の自己署名証明書の内容を表示させます。

「知事の証明書」をクリックします。

ログインダイアログボックスが現れるので、パスワードを入力し、「OK」をクリックします。

フィンガープリントに関して、先に入手した「電子証明書の利用のご案内」等に記載された、都道府県知事（都道府県認証局）の自己署名証明書のフィンガープリントと一致するかどうか確認します。

「詳細情報」タブをクリックします。

尚、都道府県知事（都道府県認証局）の自己署名証明書は、利用者が地方行政機関とオンラインでやり取りする際に、地方行政機関の真正性を検証するのに使用されます。

スクロールして、「項目名」と「値」を確認します。

「項目名」をクリックすると、
下の窓に、その詳細内容が表示されます。

確認し終わったら、証明書表示のウインドウを閉じます。